(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 22 946 A 1**

(51) Int. Cl.[7]:
G 07 C 11/00
H 04 L 9/06

(21) Aktenzeichen: 199 22 946.5
(22) Anmeldetag: 14. 5. 1999
(43) Offenlegungstag: 23. 11. 2000

DE 199 22 946 A 1

(71) Anmelder:
Daimler Chrysler AG, 70567 Stuttgart, DE

(72) Erfinder:
Ueberberg, Johannes, Dr., 53757 Sankt Augustin, DE; Welschenbach, Michael, Dipl.-Math., 51143 Köln, DE

(56) Entgegenhaltungen:

DE	196 48 767 A1
DE	39 27 270 A1
FR	27 31 536 A1
US	57 87 172
EP	07 30 253 A2
WO	98 52 162 A2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Einbringen von Authentikationsdaten auf eine Hardwareeinheit

(57) Beim vorliegenden Verfahren zum Einbringen von Authentikationsdaten auf eine Hardwareeinheit, die wenigstens einen privaten Schlüssel enthält, werden die außerhalb der Hardwareeinheit vorliegenden Authentikationsdaten mit dem öffentlichen Schlüssel außerhalb der Hardwareeinheit verschlüsselt und anschließend an die Hardwareeinheit übertragen. Durch diese Maßnahmen ist eine größtmögliche Sicherheit bezüglich der Übertragung der Authentikationsdaten gewährleistet.

DE 199 22 946 A 1

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren zum Einbringen von Authentikationsdaten auf eine Hardwareeinheit, die wenigstens einen privaten Schlüssel enthält.

Zur Absicherung eines elektronischen Datenverkehrs wird zunehmend asymmetrische Kryptographie eingesetzt. Das Kennzeichen der asymmetrischen Kryptographie ist der Einsatz eines Schlüsselpaars, bestehend aus einem geheimen privaten Schlüssels sowie einem öffentlichen allgemein zugänglichen Schlüssel.

Die Schlüsselpaare werden für praktisch alle Maßnahmen zur Sicherung elektronischer Daten eingesetzt: Beispiele hierfür sind Signaturen, Integritätsschutz, Vertraulichkeit, Verschlüsselung, Identitätsnachweis, Authentikation, Zertifikatproduktion, Copyrightschutz, und vieles mehr.

Zunehmend werden die privaten Schlüssel in speziellen Hardwareeinheiten erzeugt und sicher gespeichert. Derartige Hardwareeinheiten sind außerdem in der Lage, Verschlüsselungen oder Signaturen auszuführen, so daß der oder die privaten Schlüssel die Hardwareeinheit zu keinem Augenblick ihrer Lebenszeit verlassen. Weder bei der Erzeugung noch bei der Speicherung noch bei der Ausführung der kryptographischen Operationen verläßt der private Schlüssel die Hardwareeinheit. Ein Beispiel für eine Infrastruktur, in der solche Hardwareeinheiten zukünftig eingesetzt werden sollen, sind die Public-Key-Infrastrukturen im Rahmen von Signaturgesetzen. Weltweit gibt es vergleichbare Infrastrukturen bzw. werden solche Infrastrukturen aufgebaut. Besonders verbreitet als Hardwareeinheiten sind Chipkarten mit Prozessoren oder PCMCIA-Karten.

An den privaten Schlüssel wird die Anforderung gestellt, daß er sicher gespeichert werden kann und bei seiner Anwendung zu kryptographischen Prozessen die Hardwareeinheit nicht verläßt.

Hardwareeinheiten bieten in der Regel einen zweifachen Schutzmechanismus. In der Hardwareeinheit sind der oder die privaten Schlüssel gespeichert. Zur Verwendung des oder der privaten Schlüssel ist also der physische Besitz der Hardwareeinheit notwendig. Der rechtmäßige Besitzer muß sich aber andererseits gegenüber der Hardwareeinheit als solcher ausweisen. In die Hardwareeinheit wird ein personenabhängiger Datensatz eingelesen, mit dem die Hardwareeinheit die Rechtmäßigkeit seines Besitzers überprüfen kann.

Hierzu kann eine PIN-Nummer vorgesehen sein. Eine geheime PIN (persönliche Indentifizierungsnummer) wird in die Karte eingelesen und dem Besitzer auf vertraulichem Wege mitgeteilt.

Durch Eingabe der PIN weist der Benutzer sich gegenüber der Hardwareeinheit als berechtigt aus.

Der Gebrauch von biometrischen Merkmalen stellt eine weitere Verfahrensweise zur Verfügung. Die Hardware verfügt über einen Mechanismus, um beispielsweise einen Fingerabdruck oder einen Abdruck der Augeniris abzunehmen. Das Ergebnis des Einlesens des biometrischen Merkmals wird mit einem internen Datensatz verglichen. Auf diese Weise wird die Berechtigung des Nutzers überprüft. Auch in diesem Szenario sind die personenbezogenen Datensätze, die in die Hardwareeinheit eingelesen werden, vertraulich in die Hardwareeinheit einzubringen.

Im folgenden werden die personenbezogenen Daten, wie PIN, Fingerabdruck oder Irismuster, Authentikationsdaten genannt.

Da der Authentikationsdatensatz der Hardwareeinheit die Entscheidung ermöglicht, ob ein Benutzer berechtigt ist den bzw. die privaten Schlüssel zu nutzen, ist die vertrauliche Behandlung des Authentikationsdatensatzes ein entscheidendes Kriterium für eine sichere Nutzung der Hardwareeinheit durch den berechtigten Benutzer oder Verbraucher. Da die Erstellung des Authentikationsdatensatzes sowie die Herstellung der Hardwareeinheit in der Regel durch verschiedene Personen bzw. Organisationen vorgenommen wird, ist das Einlesen des Authentikationsdatensatzes in die Hardwareeinheit mit besonderer Aufmerksamkeit zu verfolgen. Der Authentikationsdatensatz darf dabei nicht in die Hände von unerwünschten dritten Personen gelangen oder überhaupt die Möglichkeit dafür vorgeben.

Der Erfindung liegt nun die Aufgabe zugrunde, ein Verfahren zum Einbringen von Authentikationsdaten auf eine Hardwareeinheit anzugeben, wobei die Hardwareeinheit wenigstens einen privaten Schlüssel enthält, bei dem ein Zugriff von unberechtigten dritten Personen auf den Authentikationsdatensatz weitestgehend vermieden werden soll.

Die Aufgabe wird gelöst durch ein Verfahren zum Einbringen von Authentikationsdaten auf eine Hardwareeinheit, die wenigstens einen privaten Schlüssel enthält, wobei gemäß der Erfindung die außerhalb der Hardwareeinheit vorliegenden Authentikationsdaten mit einem dem privaten Schlüssel zugeordneten öffentlichen Schlüssel außerhalb der Hardwareeinheit verschlüsselt werden und anschließend an die Hardwareeinheit übertragen werden, wo sie mit dem dort gespeicherten geheimen Schlüssel entschlüsselt werden.

Mit dem vorliegenden erfindungsgemäßen Verfahren ist ein vertrauliches Einlesen der Authentikationsdaten in die Hardwareeinheit gewährleistet. Keine dritte Person hat die Möglichkeit, sich in den Besitz der Authentikationsdaten zu bringen, da der zum Entschlüsseln notwendige private Schlüssel ausschließlich in der Hardwareeinheit vorhanden ist.

Vorzugsweise wird wenigstens einer der beiden Schlüssel innerhalb der Hardwareeinheit erzeugt. Durch diese Maßnahme ist eine zusätzliche Sicherheit gewährleistet, da beispielsweise bei der Erzeugung des privaten Schlüssels innerhalb der Hardwareeinheit gewährleistet ist, daß der private Schlüssel zu keinem Zeitpunkt auch während seiner Benutzung außerhalb der Hardwareeinheit vorliegt.

Vorzugsweise kann als Hardwareeinheit eine Chipkarte vorgesehen sein. Der Einsatz einer Chipkarte hat sich in der Praxis besonders bewährt.

In einer weiteren Ausgestaltung sind als Authentikationsdaten PIN-Nummern vorgesehen. Die Angabe einer PIN-Nummer gewährleistet einen einfachen Zugang für eine benutzerfreundliche Hardwareeinheit.

Insbesondere sind als Authentikationsdaten biometrische Daten vorgesehen. Biometrische Daten erweisen sich in diesem Zusammenhang als besonders fälschungssicher. Außerdem ist eine eindeutige Identifizierung des Benutzers der Hardwareeinheit mit Hilfe von biometrischen Daten gewährleistet.

Vorzugsweise kann mit den Authentikationsdaten zugleich ein Zertifikat übertragen werden. Das Zertifikat beurkundet, daß der private Schlüssel tatsächlich dem Benutzer der entsprechenden Hardwareeinheit zuzuordnen ist.

Bei einer weiteren Ausgestaltung der Erfindung wird zur Sicherung der Daten ein Transportschlüssel verwendet. Dadurch wird das erfindungsgemäße Verfahren mit weiteren Sicherheitsmechanismen ausgestaltet.

Weitere vorteilhafte Ausgestaltungen sind in den Unteransprüchen wiedergegeben.

Der Prozeß des Einlesens von personenbezogenen Daten – insbesondere von Authentikationsdaten – in eine Hardwareeinheit wird als Personalisierung bezeichnet.

Typischerweise werden während der Personalisierung neben den Authentikationsdaten weitere Daten, zum Beispiel

Namen, spezielle Seriennummern oder ähnliches, eingelesen. Ferner ist die elektrische Personalisierung oft mit der optischen Personalisierung (Aufdruck von Namen, Fotos oder ähnlichem) verknüpft.

Die Hardwareeinheit weist wenigstens einen privaten Schlüssel auf. Beim vorliegenden Verfahren zum Einbringen von Authentikationsdaten in die Hardwareeinheit werden die Authentikationsdaten außerhalb der Hardwareeinheit mit dem öffentlichen Schlüssel aus der Hardwareeinheit außerhalb derselbigen verschlüsselt. Anschließend werden die mit dem öffentlichen Schlüssel verschlüsselten Authentikationsdaten auf die Hardwareeinheit übertragen bzw. in selbige eingelesen und dort mit dem in der Hardwareeinheit gespeicherten geheimen Schlüssel entschlüsselt.

Es gibt somit eine Rollentrennung zwischen der personalisierenden Stelle und derjenigen Stelle, die über den Authentikationsdatensatz verfügt bzw. ihn erstellt. Die personalisierende Stelle wird als Personalisierungsstelle bezeichnet. Die Stelle, die über die Authentikationsdaten verfügt, wird als Trusted Party bezeichnet.

Folgende Szenerien im Zusammenspiel mit Personalisierungsstelle und Trusted Party sind typisch. Die Personalisierungsstelle wird von einem Chipkarten-Hersteller betrieben. Die Trusted Party ist ein Trust-Center bzw. eine Zertifizierungsstelle. Die privaten Schlüssel werden auf den Chipkarten des Chipkarten-Herstellers erzeugt und gespeichert. Das Trust-Center beliefert die Personalisierungsstelle des Kartenherstellers mit den Authentikationsdaten.

Die Personalisierungsstelle kann auch eine – erweiterte – Registrierungsstelle sein, wo ein Kunde bzw. Benutzer eine Chipkarte mit privaten Schlüsseln und den zugehörigen Zertifikaten beantragt. Die Trusted Party ist wiederum ein Trust-Center bzw. eine Zertifizierungsstelle, die der Registrierungsstelle die Authentikationsdaten zum Einlesen in die Chipkarte liefert.

Eine dritte Variante besteht darin, daß sowohl die Personalisierungsstelle als auch die Trusted Party durch ein Trust-Center betrieben werden, das intern die Rollen Personalisierungsstelle und Trusted Party trennt.

Unabhängig von dem vorgegebenen Szenario ist mit dem erfindungsgemäßen Verfahren gewährleistet, daß die Authentikationsdaten keiner dritten unerwünschten Person zur Verfügung stehen oder in seine Hände gelangen. Es ist somit ein größtmögliches Maß an Sicherheit für die Geheimhaltung des Authentikationsdatensatzes gewährleistet. Da die Authentikationsdaten mit dem öffentlichen Schlüssel der Hardwareeinheit verschlüsselt werden und sich der zum Entschlüsseln notwendige private Schlüssel nur in der Hardwareeinheit befindet, können die Authentikationsdaten nur in der Hardwareeinheit entschlüsselt werden. Aufgrund der internen Mechanismen der Hardwareeinheit kann der private Schlüssel der Hardwareeinheit nur von den Personen genutzt werden, die über die Trusted Party rechtmäßig in den Besitz der Authentikationsdaten gelangen. Ein Zugriff von unerwünschten dritten Personen auf die Authentikationsdaten ist nahezu unmöglich.

Zentraler Punkt der Erfindung ist somit die Verschlüsselung der Authentikationsdaten mit dem zuvor aus der Hardwareeinheit ausgelesenen öffentlichen Schlüssel sowie das Senden dieses verschlüsselten Datensatzes über die Personalisierungsstelle an die Hardwareeinheit. Die Personalisierungsstelle liest den oder die öffentlichen Schlüssel aus der Hardwareeinheit aus und sendet sie an die Trusted-Party. Die Trusted-Party erstellt die Zertifikate, welche die Zugehörigkeit des privaten Schlüssels zum entsprechenden Benutzer beglaubigen. Die Authentikationsdaten werden mit einem der öffentlichen Schlüssel, die zuvor aus der Hardwareeinheit ausgelesen wurden, von der Trusted-Party verschlüsselt und in dieser verschlüsselten Form an die Personalisierungsstelle geschickt. Die Personalisierungsstelle liest den verschlüsselten Datensatz, der in einer weiteren Ausgestaltung zugleich mit dem Zertifikat übersendet wird, in die Hardwareeinheit ein. In der Hardwareeinheit werden die verschlüsselten Authentikationsdaten mit Hilfe des zugehörigen privaten Schlüssels entschlüsselt.

Das Verfahren kann mit weiteren Sicherungsmechanismen versehen werden. In einer weiteren Ausgestaltung ist der Einsatz eines Transportschlüssels zum Übertragen der Daten vorgesehen. Des weiteren kann bei der Verwendung von Chipkarten ein kartenspezifischer Identifikationsschlüssel verwendet werden.

Als Hardwareeinheit sind neben dem Einsatz einer Chipkarte auch alle anderen möglichen Ausführungsformen einer Hardwareeinheit denkbar. PIN-Nummern und biometrische Daten, insbesondere die Abdrücke von Fingern oder der Augeniris, sind als Authentikationsdaten besonders geeignet. Darüber hinaus sind aber alle anderen möglichen Ausführungsformen von Authentikationsdaten für dieses Verfahren einsetzbar.

Die Übertragung der Authentikationsdaten kann mit allen bekannten öffentlichen Netzen zum Verbreiten von Daten durchgeführt werden.

Das erfindungsgemäße Verfahren hat den Vorteil, daß die Authentikationsdaten im Sinne der Ende-Zu-Ende-Sicherheit vertraulich in die Hardwareeinheit eingelesen werden. Kein dritter Außenstehender, insbesondere auch nicht die Personalisierungsstelle, hat die Möglichkeit, sich in den Besitz der Authentikationsdaten zu bringen, da der zum Entschlüsseln notwendige private Schlüssel ausschließlich in der Hardwareeinheit zur Verfügung steht. Die Sicherheit des Verfahrens wird dadurch erweitert, daß sinnvollerweise der private- und der öffentliche Schlüssel in der Hardwareeinheit generiert werden.

Das folgende Szenario wird zukünftig von besonderer Bedeutung sein:

- die Hardwareeinheiten sind Chipkarten,
- die Authentikationsdaten sind PINS,
- die Trusted-Party ist ein Trust-Center oder eine Zertifizierungsstelle,
- die Personalisierungsstelle ist Teil des Trust-Centers oder eine Organisationseinheit eines Kartenherstellers oder eine Registrierungsstelle, die die Teilnehmerdaten aufnimmt und die Chipkarten personalisiert und ausgibt.

Patentansprüche

1. Verfahren zum Einbringen von Authentikationsdaten auf eine Hardwareeinheit, die wenigstens einen privaten Schlüssel enthält, **dadurch gekennzeichnet**, daß die außerhalb der Hardwareeinheit vorliegenden Authentikationsdaten mit einem öffentlichen Schlüssel außerhalb der Hardwareeinheit verschlüsselt werden und anschließend an die Hardwareeinheit übertragen werden.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der private und der öffentliche Schlüssel innerhalb der Hardwareeinheit erzeugt werden.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß als Hardwareeinheit eine Chipkarte vorgesehen wird.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß als Authentikationsdaten PIN-Nummern vorgesehen werden.

5. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß als Authentikationsdaten biometrische Daten vorgesehen werden.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß als biometrische Daten der Abdruck eines Fingers vorgesehen wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß mit den Authentikationsdaten ein Zertifikat übertragen wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß zur Sicherung der Daten ein Transportschlüssel verwendet wird.

9. Verfahren nach einem der Ansprüche 3 bis 8, dadurch gekennzeichnet, daß zur Sicherung der Daten ein kartenspezifischer Identifikationsschlüssel verwendet wird.